UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
(CHARLESTON DIVISION)

BERNARD PRIOLEAU and KATHY PRIOLEAU, individually and on behalf others similarly situated,	)	
Plaintiffs,	)	**CASE NO. 2:19-cv-1116-RMG**
v.	)	**CLASS ACTION**
ASCENSION DATA & ANALYTICS, LLC,	)	**JURY TRIAL DEMANDED**
Defendant.		

CLASS ACTION COMPLAINT

Plaintiffs, BERNARD PRIOLEAU and KATHY PRIOLEAU ("Plaintiffs"), bring this action against Defendant ASCENSION DATA & ANALYTICS, LLC ("Ascension" or "Defendant"), a Delaware limited liability company, on behalf of themselves and all others similarly situated to obtain damages, restitution and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF ACTION

1. Plaintiffs bring this class action against Defendant for failing to secure and safeguard the personally identifiable information ("PII") and mortgage and credit information that Defendant collected and maintained (collectively "Private Information"), and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been stolen and precisely what types of information were stolen (the "Data Breach").

2. Due to Defendant's negligence, the Private Information that Defendant collected and maintained could now be in the hands of thieves. Accordingly, Plaintiffs bring this action against Defendant asserting claims for negligence, violation of state data breach acts, Violation of the Fair Credit Reporting Act, and Intrusion Upon Seclusion.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d), the class contains members of diverse citizenship from Defendant, and the amount in controversy exceeds $5 million.

5. This Court has personal jurisdiction over Defendant because portions of the conduct at issue in this case occurred, among other locations, in South Carolina, and because Defendant's contacts with this district are sufficient to subject it to personal jurisdiction in this District.

6. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial portion of the events or omissions giving rise to this action occurred in this District, and the Data Breach affected consumers in this District.

PARTIES

7. Plaintiffs Bernard Prioleau and Kathy Prioleau are, and at all times mentioned herein were, individual citizens of the State of South Carolina residing in Saint Stephen, South Carolina.

8. Defendant Ascension is a Delaware limited liability corporation with its principal place of business in Fort Worth, Texas.

ASCENSION'S BUSINESS

9. Plaintiff provided information and documents in connection with a home mortgage loan to Stanwich Mortgage Acquisition Company, LLC, dba Stanwich Mortgage Loan Trust, a Delaware limited liability company.

10. Defendant is a data and analytics company for the financial industry. Part of Defendant's services include converting paper documents and hand-written notes to computer-readable files through a process known as "optical character recognition" ("OCR").[1]

11. Defendant hired OpticsML, a New York-based company, to assist with Ascension's OCR processing of documents related to mortgage and loan applications and to store the converted loan data on its servers.

THE DATA BREACH

12. Plaintiffs bring this suit on behalf of themselves and a Class of similarly situated individuals against Defendant for Defendant's failure to secure and protect Plaintiffs' and Class members' personal and financial information.

13. In January 2019, several media outlets reported that more than 24 million financial and banking documents related to tens of thousands of loans and mortgages from some of the biggest banks in the United States were made public online.[2]

14. On January 10, 2019, independent security researcher Bob Diachenko discovered a server running an Elasticsearch database that contained loan and mortgage documents, repayment schedules and other highly sensitive financial and tax documents that included personal details such as names, dates of birth and social security numbers. The

[1] *See* https://techcrunch.com/2019/01/23/financial-files/ (last visited April 12, 2019).
[2] *Id.*

server was not locked nor protected with a password, allowing anyone to access and read the massive cache of documents.[3] The exposed data appears to have come from documents Defendant processed using OCR.

15. The server contained more than a decade's worth of data. The compromised documents included loan and mortgage agreements, repayment schedules, and tax documents.

16. On information and belief, Stanwich and other financial institutions provided the financial and banking documents to Ascension for data analysis and portfolio valuations. Ascension then hired OpticsML to scan the documents.

17. Upon discovery of the database, Diachenko sent an email to CitiFinancial ("Citi) on January 10, 2019 to inform them of the discovery of the mortgage and loan documents that originated with Citi.

18. Ascension and Stanwich confirmed the breach occurred and represented that two cloud-servers belonging to OpticsML were subject to unauthorized access by foreign IP addresses in the Data Breach. *See* **Exhibit A**, Notice of Ascension Data Breach letter ("Notice").

19. The unauthorized access of the personal and financial information could have been acquired as early as February 2018 until January 2019. *Id*.

20. On January 15, 2019, OpticsML learned of a server configuration error that may have led to the exposure of some mortgage-related documents. OpticsML immediately shut down the server in question and secured the data.

[3] *See, e.g., id.*

21. After the database was shut down, on January 11, 2019, Diachenko found a second Amazon S3 storage server whose permissions had been set to public from the default private settings.[4]

22. The Amazon S3 storage server contained 21 files containing 23,000 pages of PDF documents stitched together. Some or all of the data was the same that had been in the storage server database that was previously shut down.

23. The files in the Amazon S3 storage server were documents from banks and financial institutions across the United States and included loans and mortgage agreements, documents from the U.S. Department of Housing and Urban Development, W-2 tax forms, loan repayment schedules, and other sensitive financial information.

24. Although Defendant was storing sensitive documents containing personal and financial information that Defendant knew were valuable and vulnerable to misuse, Defendant was negligent in protecting the personal and financial information.

25. Despite the unauthorized access to the two cloud servers by foreign IP addresses as early as February 2018, which Ascension and Stanwich claim to have only learned about on January 15, 2019, notice was not mailed to Plaintiff and other Class members regarding the Data Breach until February 14, 2019.

26. The Notice that Plaintiffs received from Stanwich and Ascension acknowledges that a collection of highly sensitive personal and financial information was subject to unauthorized access by foreign IP addresses. Even though Plaintiffs and Class members are now at a high risk of identity theft for many years to come, the Notice offers Plaintiffs credit monitoring and identity theft protection services for only two years.

[4] *See* https://techcrunch.com/2019/01/24/mortgage-loan-leak-gets-worse/ (last visited April 12, 2019).

Plaintiffs and Class members were also advised to be vigilant and review their credit reports for suspected incidents of identify theft, and to educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

DATA BREACHES PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

27. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[5]

28. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[6]

29. Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

30. Identity thieves can also use SSNs to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's

[5] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," pg. 2, by U.S. Government Accountability Office, June 2007, at: https://www.gao.gov/new.items/d07737.pdf (last visited April 12, 2019) ("GAO Report").
[6] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

31. What's more, there may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at page 29.

32. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

33. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

34. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

35. Plaintiffs and members of the Class have suffered or will suffer actual injury as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to

their account funds and costs associated with the inability to obtain money from their accounts, and damage to their credit, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Contacting their financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

36. Moreover, Plaintiffs and the Class members have an interest in ensuring that their personal and financial information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards,

including making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

37. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ALLEGATIONS

38. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

39. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All individuals whose personally identifiable information and/or financial information was provided to Ascension Data & Analytics LLC and compromised in the Data Breach. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

40. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is in the millions.

41. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a) Whether Defendant unlawfully used, maintained, lost or disclosed Class members' personal and/or financial information;

b) Whether Defendant unreasonably delayed in notifying affected customers of the Data Breach and whether the belated notice was adequate;

c) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

d) Whether Defendant's conduct was negligent;

e) Whether Defendant violated the requirements of South Carolina Code § 39-1-90 *et al.* (2009);

f) Whether Defendant's acts and practices complained of herein amount to acts of intrusion upon seclusion under the law of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia;

g) Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

22. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by Defendant.

23. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

24. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

25. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

26. Defendant has acted or refused to act on grounds that apply generally to the Class, as alleged above, and certification is proper under Rule 23(b)(2).

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiffs and All Class Members)

51. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

52. Plaintiffs bring this claim individually and on behalf of the nationwide Class.

53. Defendant knowingly collected, came into possession of and maintained Plaintiffs' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

54. Defendant had and continues to have a duty to timely disclose that Plaintiffs' Private Information within its possession might have been compromised and precisely the types of information that were compromised.

55. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' Private Information.

56. Defendant systematically failed to provide adequate security for data in its possession.

57. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs by failing to exercise reasonable care in protecting and safeguarding Plaintiff's Private Information within Defendant's possession.

58. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' Private Information.

59. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class members the fact that their Private Information within its possession might have been compromised and precisely the type of information compromised.

60. Defendant's breach of duties owed to Plaintiff and the Class proximately caused Plaintiffs' and Class members' Private Information to be compromised.

61. As a result of Defendant's ongoing failure to notify consumers regarding what type of PII has been compromised, consumers are unable to take the necessary precautions to mitigate their damages by preventing future fraud.

62. Defendant's breaches of duty caused Plaintiffs to suffer from identity theft, phishing, loss of time and money to monitor their finances for fraud, and loss of control over their PII.

63. As a result of Defendant's negligence and breach of duties, Plaintiffs are in danger of imminent harm that their PII, which is still in the possession of third parties, will be used for fraudulent purposes.

64. Plaintiffs seek the award of actual damages on behalf of the Class.

65. In failing to secure Plaintiffs' and Class Members' Private Information and promptly notifying them of the Data Breach, Defendant was guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights. Plaintiffs therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

66. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to consumer information and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII have been compromised as a result of the data breach.

SECOND COUNT
Violation of State Data Breach Acts
(On Behalf of Plaintiffs and All Class Members Who Reside in the Data Breach Statute States)

67. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

68. Defendant owns, licenses and/or maintains computerized data that includes Plaintiffs' and Class Members' PII.

69. Defendant was required to, but failed, to take all reasonable steps to dispose, or arrange for the disposal, of records within its custody or control containing personal information when the records were no longer to be retained, by shredding, erasing, or otherwise modifying

the personal information in those records to make it unreadable or undecipherable through any means.

70. Defendant's conduct, as alleged above, violated the data breach statutes of many states (the "Data Breach Statute States"), including:

a. California, Cal. Civ. Code §§ 1798.80 *et. seq*.;

b. Hawaii, Haw. Rev. Stat. § 487N-1–4 (2006);

c. Illinois, 815 Ill. Comp Stat. Ann. 530/1–/30 (2006);

d. Louisiana, La. Rev. Stat. § 51:3071-3077 (2005), and L.A.C. 16:III.701;

e. Michigan, Mich. Comp. Laws Ann. §§ 445.63, 445.65, 445.72 (2006);

f. New Hampshire, N.H. Rev. Stat. Ann. §§ 359-C:19–C:21, 358-A:4 (2006)., 332-I:1–I:610;

g. New Jersey, N.J. Stat. Ann. § 56:8-163–66 (2005);

h. North Carolina, N.C. Gen. Stat. §§ 75-65 (2005); as amended (2009);

i. Oregon, Or. Rev. Stat. §§ 646A.602, 646A.604, 646A.624 (2011);

j. Puerto Rico, 10 L.P.R.A. § 4051; 10 L.P.R.A. § 4052 (2005), as amended (2008);

k. South Carolina, S.C. Code § 1-11-490 (2008); S.C. Code § 39-1-90 (2009);

l. Virgin Islands, 14 V.I.C. § 2208, et seq. (2005);

m. Virginia, Va. Code Ann. § 18.2-186.6 (2008); Va. Code Ann. § 32.1– 127.1:05 (2011); and

n. the District of Columbia, D.C. Code § 28-3851 to 28-3853 (2007) (collectively, the "State Data Breach Acts").

71. Defendant was required to, but failed, to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

72. The Data Breach constituted a "breach of the security system" within the meaning of section 39-1-90(D) of the South Carolina Code, and other State Data Breach Acts.

73. The information compromised in the Data Breach constituted "personal identifying information" within the meaning of section 39-1-90(D) of the South Carolina Code, and other State Data Breach Acts.

74. Like other State Data Breach Acts, South Carolina Code § 39-1-90(A) requires disclosure of data breaches "in the most expedient time possible and without unreasonable delay…."

75. Defendant violated South Carolina Code § 39-1-90(A) and other State Data Breach Acts by unreasonably delaying disclosure of the Data Breach to Plaintiffs and other Class Members, whose PII was, or was reasonably believed to have been, acquired by an unauthorized person.

76. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiffs and Class Members would impede a criminal investigation.

77. As a result of Defendant's violation of State Data Breach Acts, including, South Carolina Code § 39-1-90, *et seq.*, Plaintiffs and Class Members incurred economic damages, including expenses associated with monitoring their personal financial information to prevent further fraud.

78. Plaintiffs, individually and on behalf of the Class, seek all remedies available under South Carolina Code § 39-1-90 and under the other State Data Breach Acts, including, but

not limited to: (a) actual damages suffered by Class Members as alleged above; (b) statutory damages for Defendant's willful and knowing violation of South Carolina Code § 39-1-90; (c) equitable relief; and (d) reasonable attorneys' fees and costs under S

79. outh Carolina Code § 39-1-90(G)(4).

80. Because Defendant was guilty of oppression, fraud or malice, in that it failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights, Plaintiffs also seek punitive damages, individually and on behalf of the Class.

THIRD COUNT
Violation of the Fair Credit Reporting Act
(15 U.S.C. § 1681, *et seq*.)
(On Behalf of Plaintiffs and All Class Members)

81. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

82. Ascension acquired and assembles consumers' financial and banking information from various financial institutions for use in its data analytics products.

83. Ascension's data analytics products constitute "consumer reports" because the information contained therein bears upon consumers' "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" and "is used or expected to be used or collected in whole or in part for the purpose of serving as a factor" in various financial institutions' credit decisions regarding those consumers. 15 U.S.C. § 1681a(d).

84. As such, Ascension is a "consumer reporting agency" ("CRA") as that term is defined by the Fair Credit Reporting Act ("FCRA") because it regularly assembles and/or evaluates consumer credit information for the purpose of furnishing consumer reports to third parties in the form of its data analytics products, and uses interstate commerce to prepare and/or furnish the reports. 15 U.S.C. § 1681a(f).

85. A central duty that the FCRA imposes upon CRAs is the duty to protect consumers' privacy by guarding against inappropriate disclosure to third parties. Specifically, 15 U.S.C. § 1681b permits a CRA to disclose consumers' information only for one of a handful of exclusively defined "permissible purposes." To ensure compliance, CRAs must maintain reasonable procedures to ensure that such third party disclosures are made exclusively for permissible purposes. 15 U.S.C. § 1681e(a).

86. Plaintiffs' and Class members' highly sensitive personal and financial information was compiled and stored on an online server that was neither locked nor password protected, but instead was open and available to the public. Therefore, the public's ability to access Plaintiffs' and Class members' information was not the result of Ascension's *inaction*, but was the result of Ascension's decision to make that information available to anyone who wished to view it.

87. Put another way, Ascension took an affirmative step to publish Plaintiffs' and Class members' highly sensitive personal and financial information to members of the public-*i.e.*, posting that information on a publicly available server-in the same way that owners of other websites publish the content thereon to members of the public. As such, the information accessed in the Data Breach was not "stolen," in the same sense that information returned as a result of a Google search is not "stolen" by the individual performing such a search.[7]

88. Based on the foregoing, each time a member of the public accessed the server on which Plaintiffs' and Class members' information was stored, Ascension furnished that person with a consumer report.

[7] To the extent that this Complaint characterizes access to this information as "unauthorized," for purposes of this Count, that term should be construed to mean that access to this information was not for a purpose authorized by 15 U.S.C. § 1681b.

89. However, because Ascension made those consumer reports available to the public at large, Ascension did not take reasonable steps to limit the dissemination of those consumer reports as required by 15 U.S.C. § 1681e(a).

90. Ascension's violations of 15 U.S.C. § 1681e(a) were willful, as Ascension knew that Plaintiffs' and Class members' highly sensitive personal and financial information was compiled and stored on an online server that was neither locked nor password protected, and that it could be accessed by members of the public at large. Even if Ascension's violations of 15 U.S.C. § 1681e(a) are not deemed to be willful, they are at the very least negligent because Ascension should have known that Plaintiffs' and Class members' highly sensitive personal and financial information was complied and stored on an online server that was neither locked nor password protected, and that it could be accessed by members of the public at large.

91. The FCRA also required CRAs to "follow reasonable procedures to assure maximum possible accuracy of the information" contained in a consumer report. 15 U.S.C. § 1681e(b).

92. As part of its data analytics services, Ascension published Plaintiffs' and Class members' consumer reports to various financial institutions.

93. However, as noted above, the highly sensitive personal and financial information compiled and maintained by Ascension could be used to perpetrate identity theft.

94. Therefore, the consumer reports that ascension published to various financial institutions were based on information that was subject to fraudulent manipulation.

95. Because Ascension did not undertake any procedures to ensure that the information in the consumer reports that it published to financial institutions was genuine-such as by securing the server on which that information was stored-Ascension did not "follow

reasonable procedures to assure maximum possible accuracy of the information" contained in Plaintiffs; and Class members' consumer reports in violation of 15 U.S.C. § 1681e(b).

96. Ascension's violations of 15 U.S.C. § 1681e(b) were willful, as Ascension knew that the information contained in Plaintiffs' and Class members' consumer reports was subject to fraudulent manipulation, but still published those consumer reports to various financial institutions anyway. Even if Ascension's violations of 15 U.S.C. § 1681e(b) are not deemed to be willful, they are at the very least negligent because Ascension should have known that the information contained in Plaintiffs' and Class members' consumer reports was subject to fraudulent manipulation, but still published those consumer reports to financial institutions anyway.

97. As a result of Ascension's willful and/or negligent violations of the FCRA, Plaintiffs and Class members have suffered and will continue to suffer actual damages, including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

98. Plaintiffs and members of the Class are entitled to recovery of actual and statutory damages, as well as attorneys' fees and costs, pursuant to 15 U.S.C. § 1681o(a) and 15 U.S.C. § 1681n(a).

FOURTH COUNT
Intrusion Upon Seclusion
(On Behalf of Plaintiffs and All Class Members)

99. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

100. Plaintiffs had a reasonable expectation of privacy in the Private Information Defendant mishandled.

101. By failing to keep Plaintiffs' Private Information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' privacy by:

a) Intruding into Plaintiffs' private affairs in a manner that would be highly offensive to a reasonable person; and

b) Publicizing private facts about the Plaintiffs, which is highly offensive to a reasonable person.

102. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Defendant's actions highly offensive.

103. Defendant invaded Plaintiffs' right to privacy and intruded into Plaintiffs' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

104. As a proximate result of such misuse and disclosures, Plaintiffs' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendants' conduct amounted to a serious invasion of Plaintiffs' protected privacy interests.

105. In failing to protect Plaintiffs' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiffs and the Class Members' rights to have such information kept

confidential and private. The Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf of themselves and the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage and safety and to disclose with specificity the type of PII compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

F. Ordering Defendant to disseminate individualized notice of the Data Breach to all Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

Dated: April 16, 2019

Respectfully submitted,

By: /s/ Harper Todd Segui

Harper Todd Segui
WHITFIELD BRYSON & MASON LLP
Federal ID No. 10841
P.O. Box 1483
Mount Pleasant, South Carolina 29465
Telephone 919.600.5000
Email: harper@wbmllp.com

KOZONIS & KLINGER, LTD.
Gary M. Klinger (*pro hac vice forthcoming*)
4849 N. Milwaukee Ave., Ste. 300
Chicago, Illinois 60630
Phone: 312.283.3814
Fax: 773.496.8617
Email: gklinger@kozonislaw.com

WHITFIELD BRYSON & MASON LLP
Gary E. Mason (*pro hac vice forthcoming)*
Danielle L. Perry
5101 Wisconsin Ave., NW
Washington, DC 20016
Phone: (202) 640-1160
Email: gmason@wbmllp.com
Email: dperry@wbmllp.com

Attorneys for Plaintiffs and the Proposed Class

Stanwich Mortgage Loan Trust

February 11, 2019

73 1 16182 ********AUTO**ALL FOR AADC 294
BERNARD PRIOLEAU
[redacted]
SAINT STEPHEN, SC [redacted]

RE: Notice of Data Breach

Dear Bernard Prioleau,

Stanwich Mortgage Loan Trust A ("Stanwich") and Ascension Data & Analytics, LLC ("Ascension") were recently notified of an event that may involve some of your personal information. This event relates to documentation associated with your mortgage loan, which is (or may have been at one time) held by Stanwich. Although we are not aware of any identity theft or fraud occurring as a result of this event, we are writing to provide you with information on the event, steps Ascension and Stanwich are taking in response, and steps you may take to better protect against the possibility of identity theft and fraud from any source, should you feel it is appropriate to do so.

What Happened? Ascension provides data analytics in connection with residential mortgage loans which are or may have been held by Stanwich. As part of its services, Ascension has custody of certain data related to the Stanwich loans and contracts with a third-party vendor, PairPrep, Inc., d/b/a OpticsML ("OpticsML") to process that data using certain technology.

On January 15, 2019, Ascension and Stanwich were informed of a potential incident involving OpticsML. An investigation, supported by third-party forensic experts, was immediately commenced to determine the nature and scope of the event. Beginning on January 25, 2019, Ascension and Stanwich confirmed that two cloud-servers belonging to OpticsML were subject to unauthorized access by foreign IP addresses, and that the data hosted on those servers could have been acquired as early as February 2018 until January 2019.

What Information Was Involved? Although the investigation is ongoing, Ascension and Stanwich determined that the following types of your information may have been on the servers, and could have been subject to unauthorized access or acquisition: name; address; Social Security number; loan information; bank account, credit, or debit card information; driver's license number; date of birth; credit file; and any other information you may have provided as part of your mortgage loan application. The types of information listed above were not necessarily impacted for everyone.

What We Are Doing. We take the protection of personal information very seriously. The information has been taken offline and law enforcement has been notified. Although a third-party (OpticsML) was in possession of the information that was exposed, and we are not aware of any identity theft or fraud occurring as a result of this event, to illustrate our commitment to the protection of personal information, we have arranged to have Kroll make available at no cost to you credit monitoring and identity theft protection services for two (2) years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to enroll and receive these services. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information" to learn more about ways to protect personal information. You may also enroll to receive the free credit monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact 877-460-5062 (toll free) Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Standard Time.

Ascension and Stanwich take the privacy and security of personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Stanwich Mortgage Loan Trust A

By Stanwich Mortgage Acquisition Company IV, LLC,
as Trust Manager for Stanwich Mortgage Loan Trust A

By 

Jason Pinson, CEO

Stanwich Mortgage Loan Trust

February 11, 2019

73 1 16180 **********AUTO**ALL FOR AADC 294
KATHY JONES PRIOLEAU
[redacted]
SAINT STEPHEN, SC [redacted]

RE: Notice of Data Breach

Dear Kathy Jones Prioleau,

Stanwich Mortgage Loan Trust A ("Stanwich") and Ascension Data & Analytics, LLC ("Ascension") were recently notified of an event that may involve some of your personal information. This event relates to documentation associated with your mortgage loan, which is (or may have been at one time) held by Stanwich. Although we are not aware of any identity theft or fraud occurring as a result of this event, we are writing to provide you with information on the event, steps Ascension and Stanwich are taking in response, and steps you may take to better protect against the possibility of identity theft and fraud from any source, should you feel it is appropriate to do so.

What Happened? Ascension provides data analytics in connection with residential mortgage loans which are or may have been held by Stanwich. As part of its services, Ascension has custody of certain data related to the Stanwich loans and contracts with a third-party vendor, PairPrep, Inc., d/b/a OpticsML ("OpticsML") to process that data using certain technology.

On January 15, 2019, Ascension and Stanwich were informed of a potential incident involving OpticsML. An investigation, supported by third-party forensic experts, was immediately commenced to determine the nature and scope of the event. Beginning on January 25, 2019, Ascension and Stanwich confirmed that two cloud-servers belonging to OpticsML were subject to unauthorized access by foreign IP addresses, and that the data hosted on those servers could have been acquired as early as February 2018 until January 2019.

What Information Was Involved? Although the investigation is ongoing, Ascension and Stanwich determined that the following types of your information may have been on the servers, and could have been subject to unauthorized access or acquisition: name; address; Social Security number; loan information; bank account, credit, or debit card information; driver's license number; date of birth; credit file; and any other information you may have provided as part of your mortgage loan application. The types of information listed above were not necessarily impacted for everyone.

What We Are Doing. We take the protection of personal information very seriously. The information has been taken offline and law enforcement has been notified. Although a third-party (OpticsML) was in possession of the information that was exposed, and we are not aware of any identity theft or fraud occurring as a result of this event, to illustrate our commitment to the protection of personal information, we have arranged to have Kroll make available at no cost to you credit monitoring and identity theft protection services for two (2) years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Please review the instructions contained in the attached "Steps You Can Take to Protect Your Information" to enroll and receive these services. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information" to learn more about ways to protect personal information. You may also enroll to receive the free credit monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact 877-460-5062 (toll free) Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Standard Time.

Ascension and Stanwich take the privacy and security of personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Stanwich Mortgage Loan Trust A

By Stanwich Mortgage Acquisition Company IV, LLC,
as Trust Manager for Stanwich Mortgage Loan Trust A

By

Jason Pinson, CEO